No. 18-56669

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNDER SEAL,

APPELLANT,

v.

WILLIAM P. BARR, ATTORNEY GENERAL,

APPELLEE.

On Appeal from the United States District Court
for the Southern District of California

Case No. 18-cv-2269-BAS-MDD
Honorable Cynthia A. Bashant, District Judge

BRIEF OF MICROSOFT, GOOGLE, APPLE, AND FACEBOOK AS *AMICI CURIAE* IN SUPPORT OF APPELLANT

Nora Puckett
GOOGLE LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043
(650) 253-0000
Counsel for Google

James M. Garland
Alexander A. Berengaut
Lauren K. Moxley
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
(202) 662-6000
Counsel for Microsoft, Apple, and Facebook

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Ninth Circuit Rules of Appellate Procedure, *amici* make the following disclosure statements:

Microsoft has no parent corporation. No publicly held corporation holds 10% or more of its outstanding common stock.

Google is an indirect subsidiary of Alphabet Inc., a publicly held company. Alphabet Inc. has no parent corporation, and no publicly held company owns 10% or more of its outstanding common stock.

Apple has no parent corporation. No publicly held corporation holds 10% or more of its outstanding common stock.

Facebook has no parent corporation. No publicly held corporation holds 10% or more of its outstanding common stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTERESTS OF *AMICI*[1]

Microsoft, Google, Apple, and Facebook ("*amici*") are leading providers of cloud computing and social media services. *Amici* are committed to notifying customers about the nature and scope of government demands for private data. One form of legal demand that *amici* receive are National Security Letters ("NSLs"), which seek private non-content information relating to specified customers. The vast majority of NSLs are accompanied by nondisclosure requirements that prohibit *amici* from disclosing the existence of the demand or its substance. *Amici* have a significant interest in opposing overbroad nondisclosure requirements, including nondisclosure requirements of indefinite duration. Indefinite nondisclosure requirements threaten to silence *amici* from notifying their customers of the nature, scope, and existence NSLs in perpetuity, even after the government's need for secrecy has ended.

Microsoft is a leader in the technology industry. Since its founding in 1975, it has developed a wide range of services, software, and hardware products, including the Office suite of productivity applications, the flagship Windows operating system, the Bing search engine, the Surface tablet computer, the Xbox

[1] This brief is filed with the consent of all parties. Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), *amici* certify that no party's counsel authored this brief in whole or in part, no party or party's counsel contributed money that was intended to fund preparing or submitting this brief, and no person—other than *amici*, their members, or their counsel—contributed money that was intended to fund preparing or submitting this brief.

gaming system, and Azure Cloud Services. These systems and services allow customers to store, access, and analyze large volumes of data.

Google is a diversified technology company whose mission is to organize the world's information and make it universally accessible and useful. Google offers a variety of web-based services and products—including Search, Gmail, Maps, YouTube, and Blogger, as well as enterprise-focused services such as Google Cloud Platform and G Suite—that are used by people and businesses throughout the United States and around the world.

Apple revolutionized personal technology with the introduction of the Macintosh in 1984. Today, Apple leads the world in innovation with iPhone, iPad, Mac, Apple Watch and Apple TV. Apple's four software platforms—iOS, macOS, watchOS and tvOS—provide seamless experiences across all Apple devices and empower people with breakthrough services, including the App Store, Apple Music, Apple Pay and iCloud.

Facebook is one of the world's leading providers of social media services. Facebook provides a free Internet-based social media service that enables more than two billion people to connect with friends and family, to build community, to discover what is going on in the world around them, and to share and publish the opinions, ideas, photos, and activities that matter to them and the people they care about.

INTRODUCTION

The Federal Bureau of Investigation ("FBI") issues NSLs to service providers for private non-content information relating to their customers. In the vast majority of those instances, the FBI simultaneously imposes a nondisclosure requirement that indefinitely prohibits the provider from notifying its customers about the NSL and its substance. At the same time, the NSL statute does not require the government to directly notify account holders when it issues an NSL. Customers therefore rely on their providers for notification of NSLs when permitted and to press the government for permission to notify when the government's need for secrecy has ended.

The record in this case reflects that, eight years ago, the FBI imposed indefinite nondisclosure requirements on a provider in connection with three NSLs. The district court below granted the government's petition to enforce the nondisclosure requirements "unless and until the Government informs it otherwise." ER10. These gag orders restrain providers' First Amendment rights to communicate with their customers about an issue of public concern: the use of NSLs to obtain private data. What is more, they threaten to do so in perpetuity.

The district court erred in enforcing NSL nondisclosure requirements of an indefinite duration without requiring the government to periodically establish a compelling ongoing need for the restriction on speech. As this Court has

recognized, NSL nondisclosure requirements are subject to strict scrutiny. *In re Nat'l Sec. Letter*, 863 F.3d 1110, 1123 (9th Cir. 2017). To satisfy strict scrutiny review, nondisclosure requirements must be narrowly tailored to promote a compelling government interest, which means they must be the least speech-restrictive means of achieving the government's purpose. *See United States v. Playboy Entm't Grp., Inc.*, 529 U.S. 803, 813 (2000).

The government has not met its burden. By definition, indefinite nondisclosure requirements last longer than is necessary to serve the government's interest in secrecy. The First Amendment demands a less restrictive alternative. This Court should vacate the district court's decision and remand the case with instructions to impose a definite, reasonable time limit on the nondisclosure requirements, and require the government to justify any further delay in disclosure.

SUMMARY OF THE ARGUMENT

I. The government has the authority to issue NSLs to third-party providers to obtain certain non-content information about particular customers. Like subpoenas, NSLs may issue without prior judicial approval. Unlike subpoenas, however, the government may simultaneously impose nondisclosure obligations that prohibit the provider in perpetuity from notifying its customer about the demand. *Amici* are committed to notifying their customers about government demands for customer data to the extent permitted by law, as is their right under

the Constitution. But NSL nondisclosure requirements of indefinite duration, like the three at issue in this case, prevent providers from exercising such rights.

II. One of the core purposes of the First Amendment is "to protect the free discussion of governmental affairs." *Mills v. State of Ala.*, 384 U.S. 214, 218 (1966). By prohibiting service providers from speaking with their customers about government surveillance requests for an indefinite time period, NSL nondisclosure requirements like those imposed on the Appellant restrict providers from engaging in this constitutionally-protected speech. Indefinite nondisclosure requirements also suppress customers' corollary rights as listeners. At a broader level, such restrictions chill the free discussion of public affairs—i.e., the exercise of a government surveillance power—which is a core value that the First Amendment was designed to protect.

III. As this Court has held, NSL nondisclosure requirements are presumptively invalid content-based restrictions subject to strict scrutiny. *In re Nat'l Sec. Letter*, 863 F.3d at 1123. NSL nondisclosure requirements are also prior restraints, which are presumptively invalid restrictions on speech subject to strict scrutiny review. *See In re Dan Farr Prods.*, 874 F.3d 590, 593 n.2 (9th Cir. 2017). To satisfy strict scrutiny review, nondisclosure requirements must be narrowly tailored to promote a compelling government interest, which means they must be

the least restrictive means of achieving the government's purpose. *Playboy*, 529 U.S. at 813.

IV. Here, the government cannot meet its burden of showing that indefinite nondisclosure requirements imposed under the NSL statute are the least speech-restrictive means to achieve its purposes. By definition, nondisclosure requirements of indefinite duration are not narrowly tailored, as they necessarily extend beyond the time period for which the government has a compelling interest in secrecy. The district court erred to the extent it concluded that this flaw was cured by the providers' ability to seek judicial review of indefinite nondisclosure requirements. The First Amendment requires nondisclosure requirements to be of limited duration, and the *government* bears the burden of periodically justifying further delay in disclosure.

ARGUMENT

I. The NSL Statute Permits the FBI to Impose Nondisclosure Obligations on Providers, Which Prevent *Amici* from Notifying Their Customers of the NSLs.

A. Cloud Computing and Social Media Permit the Government to Serve Legal Demands on the Provider Rather Than the Customer.

Today, most individuals and enterprises store data in the "cloud"— a network of remote servers that continuously transfer data back and forth to digital devices. *See Riley v. California*, 573 U.S. 373, 397 (2014). The term "cloud" also encompasses services such as web-based email services, instant messaging, and

content hosting. A cloud or social media customer's personal computer, mobile phone, or other digital device is "a conduit to retrieving information from the cloud, akin to the key to a safe deposit box." *United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013) (en banc). As a result, people entrust providers with sensitive data, including private documents, emails, messages, photographs, personal information, and business correspondence. People also entrust providers with private account information about themselves, such as their name, address, email address, length of service, and method of payment.

The government may serve compulsory legal process on providers; at the same time, it may impose a nondisclosure requirement barring the provider from disclosing the existence of the demand or the data that it seeks. As a result, targets of digital investigations often do not know when the government has obtained their private information from a provider.

B. The NSL Statute Permits the FBI to Issue NSLs and Nondisclosure Requirements on Providers.

NSLs are one type of legal demand that the government can serve on providers without any prior judicial approval. Specifically, an NSL is an administrative subpoena issued by the FBI to "[a] wire or electronic communication service provider" for "subscriber information and toll billing records information." 18 U.S.C. § 2709(a). The FBI uses NSLs to obtain the email addresses associated with accounts, screen names, billing records, methods

of payment, and subscriber information associated with particular email addresses such as names, addresses, and length of service.[2]

To obtain an NSL, the FBI need only obtain self-certification by a high-ranking FBI official. 18 U.S.C. § 2709(b). The FBI official may also impose a nondisclosure requirement on an NSL recipient, prohibiting the recipient from disclosing the contents or existence of the NSL, without prior judicial approval. *Id.* § 2709(c). An NSL recipient is required to comply with the request, subject to the availability of judicial review. *Id.* §§ 2709(a), 3511(b).

In 2015, Congress enacted the USA FREEDOM Act, Pub. L. No. 114-23, § 502(g), 129 Stat. 268, 288-89 ("USA Freedom Act"). Among other things, the USA Freedom Act amended the judicial review procedures for NSL nondisclosure requirements. Under the amended statute, when an NSL recipient notifies the government that it desires judicial review of a nondisclosure requirement, the FBI is required to apply to the district court for a nondisclosure order and certify that the nondisclosure obligation remains justified. *See* USA Freedom Act, § 503 (codified at 18 U.S.C. § 3511(b)(1)).

The USA Freedom Act also required the Attorney General to adopt "procedures with respect to nondisclosure requirements" to establish, *inter alia*,

[2] *See A Review of the Federal Bureau of Investigation's Use of National Security Letters*, Office of the Inspector General xii (Mar. 2007, publicly released Feb. 2016), https://oig.justice.gov/reports/2016/NSL-2007.pdf.

"the review at appropriate intervals of such a nondisclosure requirement to assess whether the facts supporting nondisclosure continue to exist." USA Freedom Act, 129 Stat. 268, 288 (codified at 12 U.S.C. § 3414 note). In response, the Attorney General adopted the FBI Termination Procedures. *See Termination Procedures for National Security Letter Nondisclosure Requirement*, Fed. Bureau of Investigation (Nov. 24, 2015). The Termination Procedures require the FBI to review a nondisclosure obligation at two discrete points in time: (1) at the closure of the underlying investigation and (2) "on the three-year anniversary of the initiation" of the investigation. *Id.* at 2. The Termination Procedures do not require the FBI to review nondisclosure requirements for NSLs issued in connection with investigations that have passed their third anniversary or closed before the effective date of the procedures. *See id.* Nor do they require any future review of NSLs when the FBI decides at the close of an investigation that the nondisclosure obligations should remain in place. *See id.*

The FBI issues thousands of NSLs and NSL nondisclosure requirements each year. Specifically, since 2015, the FBI has issued between 12,150 and 12,870 NSLs per calendar year.[3] Nearly all NSLs are accompanied by nondisclosure

[3] *See Statistical Transparency Report: Regarding Use of National Security Authorities*, Dir. of Nat'l Intelligence (Apr. 2018), https://www.dni.gov/files/documents/icotr/2018-ASTR----CY2017----FINAL-for-Release-5.4.18.pdf.

obligations that prevent the provider from disclosing the content or even existence of an NSL.[4] And it appears the FBI has lifted nondisclosure obligations associated with NSLs in only a small number of instances relative to the overall volume of NSLs. Based on published transparency reports, the FBI has only lifted one NSL nondisclosure requirement for Microsoft, one for Apple, thirty-three for Facebook, and forty for Google.[5]

C. Providers Are Committed to Notifying Their Customers About Government Demands for Data.

As the U.S. Chamber of Commerce has explained, when individuals and business customers of cloud services are not informed of government demands,

[4] *See, e.g.*, *In re Nat'l Sec. Letter*, 930 F. Supp. 2d 1064, 1074 (N.D. Cal. 2013) ("A review of the FBI's use of NSLs discloses that the FBI issued nondisclosure orders for 97% of the NSLs it had issued"); *accord Reauthorizing the USA Patriot Act: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. 6 (2009) (statement of Glenn Fine, Inspector Gen., Dep't of Just.), www.justice.gov/oig/testimony/t0909.pdf (In a "random sample of NSLs," 97% of the NSLs imposed nondisclosure and confidentiality requirements).

[5] *See U.S. National Security Orders Report*, Microsoft, https://www.microsoft.com/en-us/corporate-responsibility/fisa; *Transparency Report*, Apple, https://www.apple.com/legal/transparency/us.html; Chris Sonderby, *Global Government Requests Report*, Facebook (April 28, 2016), https://newsroom.fb.com/news/2016/04/global-government-requests-report-5/; Chris Sonderby, *Reinforcing Our Commitment to Transparency*, Facebook (Dec. 18, 2017), https://newsroom.fb.com/news/2017/12/reinforcing-our-commitment-to-transparency/; Chris Sonderby, *Reinforcing our Commitment to Transparency*, Facebook (May 15, 2018), https://newsroom.fb.com/news/2018/05/transparency-report-h2-2017/; Chris Sonderby, *Our Continued Commitment to Transparency*, Facebook (Nov. 15, 2018), https://newsroom.fb.com/news/2018/11/updated-transparency-report/; *United States National Security Requests*, Google, https://transparencyreport.google.com/user-data/us-national-security.

they may "be reluctant to store information in the cloud."[6] Responding to this customer interest in notification, *amici* have all committed to notify their customers when the government seeks their data, to the extent permitted by law.[7]

One way *amici* are currently permitted to speak with their customers in broad terms about their receipt of NSLs is by publishing reports that disclose aggregate information about the government's requests for customer data. As permitted under 50 U.S.C. § 1874, *amici*'s semiannual reports include aggregate data concerning NSLs in bands of 500.[8] *Amici* also comment on this aggregate

[6] Amicus Brief, *Microsoft Corp. v. United States Dep't of Justice*, (W.D. Wash. No. 2:16-cv-00538-JLR), ECF No. 57 at 6 (supporting Microsoft's challenge to indefinite nondisclosure orders issued in conjunction with legal process under the Stored Communications Act).

[7] *See About Our Practices and Your Data*, Microsoft, https://blogs.microsoft.com/datalaw/our-practices/#does-microsoft-notify-users; *U.S. National Security Orders Report*, Microsoft, https://www.microsoft.com/en-us/corporate-responsibility/fisa ("Microsoft adheres to the same principles" for responding to law enforcement and national security demands "for user data and does so across all Microsoft services."); *Government Requests for Cloud Customer Data*, Google Cloud, https://cloud.google.com/security/transparency/govt-requests/; *Legal Process Guidelines*, Apple, at 6 https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf (also providing exceptions to notice where notice would create the risk of injury or death to an identifiable individual, in situations where the case relates to child endangerment, or where notice is not applicable to the underlying facts of the case); *Information for Law Enforcement Authorities*, Facebook, https://www.facebook.com/safety/groups/law/guidelines/ (also providing exceptions to notice in situations such as "child exploitation cases, emergencies or when notice would be counterproductive").

[8] *See U.S. National Security Orders Report*, Microsoft, https://www.microsoft.com/en-us/corporate-responsibility/fisa; *United States National Security Requests*, Google, https://transparencyreport.google.com/user-data/us-national-security?hl=en; *United States, National Security Letters*, Facebook, https://transparency.facebook.com/government-data-

information, to the extent legally permitted. For example, Microsoft and Facebook have published blog posts updating their customers when NSL nondisclosure requirements have been lifted following the USA Freedom Act.[9] Even prior to the statutory changes allowing publication of certain statistics about national security legal process, Google published statistics about its receipt of NSLs.[10] And in describing the current bands used for transparency reporting in the national security context, Apple explained that though it "want[s] to be more specific, these are currently the ranges and level of detail permitted under USA Freedom for reporting U.S. National Security requests."[11]

D. The NSL Nondisclosure Requirements at Issue Here May Stay in Place Forever.

In 2011, the FBI issued three NSLs to the provider in this case, all of which were accompanied by nondisclosure requirements of an indefinite duration. *See*

---

requests/country/US; *Transparency Report*, Apple, https://www.apple.com/legal/transparency/us.html.

[9] *See, e.g.*, Steve Lippman, *Microsoft Releases Biannual Transparency Reports*, Microsoft (Apr. 13, 2017), https://blogs.microsoft.com/on-the-issues/2017/04/13/microsoft-releases-biannual-transparency-reports/#sm.0000851atg8s9fdupjb20xjpmn3ss; Chris Sonderby, *Reinforcing Our Commitment to Transparency*, Facebook (Dec. 18, 2017), https://newsroom.fb.com/news/2017/12/reinforcing-our-commitment-to-transparency/.

[10] *See Transparency Report: Shedding More Light on National Security Letters*, Google (Mar. 5, 2013), https://googleblog.blogspot.com/2013/03/transparency-report-shedding-more-light.html.

[11] *About Apple's Transparency Report*, Apple, https://www.apple.com/legal/transparency/about.html.

ER42-46, 48-52, 54-58. Given the age of these NSLs, their accompanying nondisclosure obligations did not undergo review at the third anniversary of case opening, because the FBI's Termination Procedures were not in place at that time. The government has also not disclosed whether any of the underlying investigations have closed, leaving unknown whether the FBI will ever review these NSLs again in the future absent a court order to do so.

In August 2018, the provider requested judicial review of the nondisclosure requirements. ER60. As required by the amended NSL statute, the FBI filed a petition for judicial review and enforcement of the NSL nondisclosure requirements. ER104-43. The FBI argued that the nondisclosure requirements should remain in place indefinitely. ER136-37. In response, the provider did not challenge the need for the nondisclosure requirement; rather, it simply challenged the indefinite duration of the restriction on constitutionally-protected speech. ER25-26.

The district court granted the government's petition to enforce the indefinite nondisclosure requirements, ordering the provider to comply with the nondisclosure requirements "unless and until the Government informs it otherwise." ER1, 10. The court acknowledged "various cases where courts have found an indefinite duration of a nondisclosure requirement [to be] inappropriate" and imposed periodic review. ER8-9. But the court reasoned that there was "no

need" to impose a periodic review of the nondisclosure requirement because of the ability of the gagged provider to seek judicial review. ER10. Under the district court's decision, the nondisclosure restriction on the provider's free speech rights may remain in place indefinitely, without any further review unless the provider subject to the nondisclosure requirement affirmatively seeks judicial review again in the future.

II. NSL Nondisclosure Requirements Restrain Core Protected Speech Under the First Amendment.

The First Amendment reflects a "profound national commitment" to the principle that "debate on public issues should be uninhibited, robust, and wide-open." *New York Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964). This commitment exists because such speech "is more than self-expression; it is the essence of self-government," *Garrison v. State of La.*, 379 U.S. 64, 74-75 (1964), and is "critical to the functioning of our democratic system," *Long Beach Area Peace Network v. City of Long Beach*, 574 F.3d 1011, 1021 (9th Cir. 2009). There is "practically universal agreement" that a principal purpose of the First Amendment "was to protect the free discussion of governmental affairs." *Mills*, 384 U.S. at 218. Accordingly, speech regarding government activity has always rested on "the highest rung of the hierarchy of First Amendment values, and is entitled to special protection." *Connick v. Myers*, 461 U.S. 138, 145 (1983).

Indefinite NSL nondisclosure requirements suppress speech on government surveillance practices—a paradigmatic public issue—in *perpetuity*, in three ways. They restrain (1) providers' rights to communicate with their customers, (2) customers' rights as listeners, and (3) the rights of the general public to receive information about and discuss governmental surveillance practices.

A. Indefinite NSL Nondisclosure Requirements Restrain the First Amendment Rights of Providers to Communicate With Their Customers on an Issue of Profound Public Concern.

Indefinite NSL nondisclosure requirements restrain the rights of providers to speak to their customers about government demands for their data—a subject of profound and legitimate concern among *amici*'s customers.

The NSL statute does not require the government to notify account holders directly when it demands their data, even when the government declines to impose or lifts a nondisclosure restriction. Customers accordingly rely on their providers for notice of legal demands whenever legally permitted and to press the government on overbroad assertions of secrecy, such as in the instance of nondisclosure restrictions that last indefinitely.

As discussed above, *amici* are committed to notifying their customers when the government seeks information about them, whenever legally permitted, and also providing transparency in the form of aggregate transparency reporting. Yet while aggregate transparency reporting sheds some light on the number of

government requests for data, it does not satisfy customers' desire to know that data about their accounts has been sought. Nor does it meet the public's desire to understand exactly how the FBI uses NSLs.

Thus, and particularly in light of the government's routine use of nondisclosure requirements to preclude providers from notifying their customers about specific legal demands, providers have challenged overbroad nondisclosure obligations, especially ones of indefinite duration. For example, Microsoft has challenged the imposition of indefinite nondisclosure requirements with respect to legal process for customer data issued under the Stored Communications Act, a matter that Google, Apple, and many other providers supported through *amici* participation. *See Microsoft v. United States Dep't of Justice*, 233 F. Supp. 3d 887, 907 (W.D. Wash. 2017). Microsoft and Google have also successfully challenged NSL nondisclosure requirements. *See* Order, *In re Nat'l Sec. Letter*, No. 2:13-1048-RAJ (W.D.Wa. May 21, 2014); *In re Nat'l Sec. Letter*, Nos. 13-3984, 14-788 (2d Cir. Sept. 23, 2014). *Amici* pressed the government for the ability to publish aggregate numbers of national security requests in their transparency reports.[12]

[12] *See* David Drummond, *Asking the U.S. Government to Allow Google to Publish More National Security Request Data*, Google (June 11, 2013), https://www.blog.google/technology/safety-security/asking-us-government-to-allow-google-to/; *Apple's Commitment to Customer Privacy*, Apple (June 16, 2013), https://www.apple.com/apples-commitment-to-customer-privacy/; *Facebook Releases New Data About National Security Requests*, Facebook, (Feb. 3, 2014), https://newsroom.fb.com/news/2014/02/facebook-releases-new-data-about-national-security-requests/; *Microsoft's U.S. Law Enforcement and National*

The fact that *amici* are corporations does not diminish their First Amendment right to communicate with their customers about government demands for their data. *See Chula Vista Citizens for Jobs & Fair Competition v. Norris*, 782 F.3d 520, 534 (9th Cir. 2015) (en banc) (recognizing that the government may not suppress political speech on the basis of the speaker's corporate identity); *First Nat. Bank of Bos. v. Bellotti*, 435 U.S. 765 (1978) (recognizing that the First Amendment extends to corporations). Nor can *amici*'s restrained speech be characterized as commercial speech warranting lesser First Amendment protections. As this Court has explained, "[c]ommercial speech is that which does no more than propose a commercial transaction." *Valle Del Sol Inc. v. Whiting*, 709 F.3d 808, 818 (9th Cir. 2013). NSL nondisclosure requirements suppress *amici* from discussing the government's efforts to secretly obtain private non-content data about customers—a subject of public concern at the core of the First Amendment. *See Mills*, 384 U.S. at 218.

B. Indefinite NSL Nondisclosure Requirements Restrain the First Amendment Rights of Customers as Listeners.

Just as providers have a First Amendment right to speak with their customers about the government's NSL practices, customers have a corollary right

Security Requests for Last Half of 2012, Microsoft (June 14, 2013), https://blogs.microsoft.com/on-the-issues/2013/06/14/microsofts-u-s-law-enforcement-and-national-security-requests-for-last-half-of-2012/.

as listeners to receive this information. "[W]here a speaker exists, as is the case here, the protection afforded is to the communication, to its source *and to its recipients both*." *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc.*, 425 U.S. 748, 756 (1976) (emphasis added). The right to receive information is "an inherent corollary of the rights of free speech and press that are explicitly guaranteed by the Constitution." *Bd. of Educ., Island Trees Union Free Sch. Dist. No. 26 v. Pico*, 457 U.S. 853, 867 (1982). This Court has similarly recognized a listener's "corresponding interest" in receiving speech from a willing speaker. *See Hrdlicka v. Reniff*, 631 F.3d 1044, 1049 (9th Cir. 2011) ("We see no reason why this well-established principle does not apply to a publisher's interest in distributing, and an inmate's corresponding interest in receiving, unsolicited literature.").

Amici are willing speakers when it comes to notifying customers about government demands for account data. And customers have a strong corollary right to be informed about the demands that concern their private information. The First Amendment rights of customers include the right to learn of the government's use of an NSL to obtain their data when the government's need for secrecy has ended. Unless the courts require the government to reassess its need for secrecy, those First Amendment rights will be sacrificed.

C. Indefinite NSL Nondisclosure Requirements Suppress Discussion of Public Affairs.

More broadly, indefinite nondisclosure requirements on providers suppress public discussion of government surveillance practices. If the government prohibits a provider indefinitely from telling its customers that they are subject to government surveillance, "the individual targets may never learn that they had been subjected to such surveillance, and this lack of information will inevitably stifle public debate about the proper scope and extent of this important law enforcement tool." *In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 882 (S.D. Tex. 2008). "By constricting the flow of information at its source," indefinite nondisclosure requirements thus restrict "the marketplace of ideas," *id.*, and the ability to take political action based on those ideas.

Aggregate transparency reporting conveys some information to the public about the FBI's exercise of its NSL authorities, but that information is limited. Aggregate transparency reporting does not convey information about precisely how the FBI uses NSLs; about the nature and scope of information requested by the FBI through NSLs; about the individuals that have been the subject of NSLs; and in some circumstances, whether a particular provider has received any NSLs at all. The public learns of that important information only when an NSL nondisclosure requirement is lifted. Without it, the public lacks the necessary

information to engage in ongoing debate about whether the FBI is using NSLs appropriately as a matter of public policy, whether elected representatives are conducting appropriate oversight of the FBI's NSL practices, and whether legislative amendments to FBI's NSL authorities (as have been introduced at times over the past several years) may be warranted or ill-advised. *See, e.g.*, S. Amdt. 4787, 114th Cong. (2016). Thus, additional public discussion about specific NSLs—beyond that permitted by aggregate transparency reporting—will inform important, active, and ongoing public dialogue.

III. NSL Nondisclosure Requirements Are Prior Restraints and Content-Based Restrictions on Speech Subject to Strict Scrutiny.

As this Court has held, NSL nondisclosure requirements are content-based restrictions on speech subject to strict scrutiny. *In re Nat'l Sec. Letter*, 863 F.3d at 1123. A content-based restriction "target[s] speech based on its communicative content." *Reed v. Town of Gilbert, Ariz.*, 135 S. Ct. 2218, 2226 (2015). Content-based restrictions can be "obvious, defining regulated speech by particular subject matter" or "more subtle, defining regulated speech by its function or purpose." *Id.* at 2227. A content-based restriction on speech is "presumptively invalid." *R.A.V. v. City of St. Paul, Minn.*, 505 U.S. 377, 382 (1992).

An NSL nondisclosure requirement is a presumptively invalid content-based restriction because it "prohibits speech about one specific issue: the recipient may not 'disclose to any person that the Federal Bureau of Investigation has sought or

obtained access to information or records' by means of an NSL." *In re Nat'l Sec. Letter*, 863 F.3d at 1123 (quoting 18 U.S.C. § 2709(c)). By singling out and suppressing speech about the contents or existence of legal process, an NSL nondisclosure requirement "'targets speech based on its communicative content,' and restricts speech based on its 'function or purpose.'" *Id.* (quoting *Reed*, 135 S. Ct. at 2226-27).

An NSL nondisclosure requirement is also a prior restraint on speech. A prior restraint is a judicial order "forbidding certain communications when issued in advance of the time that such communications are to occur." *Alexander v. United States*, 509 U.S. 544, 550 (1993) (quotations omitted). A prior restraint is "the most serious and the least tolerable infringement on First Amendment rights." *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976). "There is a heavy presumption against prior restraints on speech, and they are subject to the strict scrutiny standard of review." *In re Dan Farr Prods.*, 874 F.3d at 593 n.2. Nondisclosure requirements are a paradigmatic example of prior restraints, as they represent "predetermined judicial prohibition[s] restraining specific expression." *In re Sealing and Non-Disclosure of Pen/Trap/2703(D) Orders*, 562 F. Supp. 2d at 882.

To satisfy strict scrutiny, nondisclosure obligations must be narrowly tailored to promote a compelling government interest, which means they must be

the least restrictive means of achieving the government's purpose. *See Playboy*, 529 U.S. at 813. The government bears the burden of demonstrating that its restriction on speech is the least restrictive means to further its purpose. *Id.* at 816-17. "When a plausible, less restrictive alternative is offered to a content-based speech restriction, it is the Government's obligation to prove that the alternative will be ineffective to achieve its goals." *Id.* at 816; *accord Askins v. U.S. Dep't of Homeland Sec.*, 899 F.3d 1035, 1045 (9th Cir. 2018) ("It is the government's burden to prove that these specific restrictions [on speech] are the least restrictive means available to further its compelling interest.").

IV. The Government Has Not Met Its Burden of Showing that the Challenged NSL Nondisclosure Requirements Are the Least Restrictive Means to Achieve Its Purposes.

The government has not demonstrated that the three indefinite nondisclosure requirements at issue here satisfy strict scrutiny. Nondisclosure requirements of indefinite duration fail strict scrutiny because, by definition, they are not narrowly tailored, i.e., they necessarily extend beyond the time needed to serve any government interest. A nondisclosure requirement that is subject to periodic review is inherently less speech-restrictive than one that extends for an unlimited duration. For example, if after a year the government's investigative interest in a target ends, any need for secrecy is also likely to end, yet an indefinite nondisclosure requirement would nevertheless continue to suppress notification in

perpetuity. In contrast, a nondisclosure requirement with a reasonable, definite time limit would necessarily terminate, allowing the provider to notify the customer of the NSL at that point.

Meanwhile, a defined-duration nondisclosure requirement that is subject to periodic review is equally effective in serving the government's legitimate interest in secrecy. With periodic review, the government's interest in nondisclosure remains protected as long as the government continues to have a compelling need for nondisclosure. So long as that need continues, the government will be able, at appropriate intervals, to convince the district court to approve an extension of the requirement. *See In re Nat'l Sec. Letters*, No. CV 16-518 (JEB), 2016 WL 7017215, at *3 (D.D.C. July 25, 2016) ("[T]riennial review fairly balances the specific burdens on the FBI against the countervailing interest that [the provider] has in avoiding a lengthy and indefinite nondisclosure bar."); *see also In re Nat'l Sec. Letter*, 165 F. Supp. 3d 352, 355 (D. Md. 2015) (finding an indefinite-duration NSL nondisclosure requirement to be problematic and mandating review every 180 days). The fact that such review may impose additional procedural burdens on the FBI cannot overcome the weighty First Amendment interests at stake.

Indeed, even the default rule for *classified* information is not indefinite secrecy. *See* Exec. Order No. 13,526, 75 Fed. Reg. 707, § 1.5(d) (Dec. 29, 2009) ("No information may remain classified indefinitely."). Instead, classified

information automatically becomes declassified after ten years, unless an exception is invoked. *Id.* § 1.5(a). Only the most sensitive classified information—information revealing the identity of a human source or "key design concepts of weapons of mass destruction"—can remain classified beyond fifty years, and only with the approval of the relevant agency head. *Id.* § 3.3(h). Just as the government is obligated to periodically review the secrecy of even the most sensitive classified information, it should be obligated to periodically review the secrecy of NSLs. Here too, in other words, the default should be eventual disclosure, not indefinite secrecy.

The unconstitutionality of indefinite nondisclosure requirements has also arisen in the analogous context of criminal legal process available under the Stored Communications Act ("SCA"), which the government can use to obtain information from providers. 18 U.S.C. § 2703. Unlike the NSL provision, however, to impose a nondisclosure obligation on a provider that has received criminal legal process under the SCA, the government must first obtain judicial approval. *Id.* § 2705(b). Several courts have recognized that indefinite nondisclosure orders issued under § 2705(b) are not narrowly tailored because they "continue to burden . . . First Amendment rights after the government's interest in keeping investigations secret dissipates." *Microsoft*, 233 F. Supp. 3d at 907; *see also Matter of Search Warrant for [redacted].com*, 248 F. Supp. 3d 970, 983 (C.D.

Cal. 2017) (reaching the same conclusion and collecting cases); *In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d at 878 ("setting a fixed expiration date on sealing and non-disclosure of electronic surveillance orders is not merely better practice, but required by . . . the First Amendment prohibition against prior restraint of speech").

The rationale of these cases applies here. Like nondisclosure requirements issued under Section 2703 of the SCA, NSL nondisclosure requirements are predetermined prohibitions on speech. *Id.* at 881. Prohibitions under either provision also "preclude speech on an entire topic"—namely, "the [accompanying] order and its underlying criminal investigations." *Id.* Just as in the SCA criminal context, indefinite NSL nondisclosure requirements will necessarily remain in place long "after the government's interest in keeping the investigation secret dissipates." *Microsoft*, 233 F. Supp. 3d at 907. In either case, a nondisclosure requirement of a reasonable limited duration is a less speech-restrictive means of achieving the government's purposes. Indeed, imposing periodic review of nondisclosure requirements is perhaps even more critical in the NSL context, where the FBI can impose nondisclosure obligations without prior judicial approval.

In permitting three NSL nondisclosure requirements to remain in place indefinitely, the district court made two critical errors. *First*, the district court

wrongly concluded that the availability of judicial review under the NSL statute relieved the government of its burden to satisfy strict scrutiny review. Under the NSL statute, if an NSL recipient requests judicial review of a nondisclosure requirement, the FBI must apply within thirty days for an order prohibiting the disclosure of the NSL and self-certify to the district court that nondisclosure is justified. *See* 18 U.S.C. §§ 3511(b)(1)(A). Based on the availability of this procedure, the district court concluded that "there is no need to impose a periodic review of the nondisclosure order" because nothing would prevent the provider "from seeking judicial review should it deem one necessary." ER10.

But the provider's ability to initiate judicial review says nothing about the *government*'s burden to satisfy strict scrutiny and impose the least speech-restrictive alternative available to achieve its purposes. *See Playboy*, 529 U.S. at 816-17. Even apart from the clear-cut constitutional requirement that the government—not private parties—bear the burden of justifying restraints on speech, requiring the provider to initiate judicial review is not practical. A provider is not privy to the government's investigation, and thus "will not know when the nondisclosure requirement's "*raison d'etre* fades." *Matter of Search Warrant for [redacted].com*, 248 F. Supp. 3d at 983. Only the government knows when the information protected by the nondisclosure obligation has become safe to disclose, such as when its investigative interest has shifted to other targets. The

district court thus erred in concluding that the providers' ability to initiate review of an NSL nondisclosure obligation was sufficient to satisfy the government's constitutional burden.

Second, the district court misapplied this Court's decision in *In re National Security Letter*. ER10. In *In re National Security Letter*, this Court rejected a *facial* constitutional challenge to the NSL statute as amended by the USA Freedom Act. 863 F.3d 1110, 1132 (9th Cir. 2017). Yet this Court's holding hinged on the fact that district courts could apply periodic review for *individual* nondisclosure obligations. *See id.* 1126-27.

Specifically, in *In re National Security Letter*, this Court made clear that "in order to ensure that the nondisclosure requirement is narrowly tailored to serve the government's compelling interest in national security, a nondisclosure requirement must terminate when it no longer serves such a purpose." *Id.* at 1126. The Court reasoned that a district court reviewing the need for nondisclosure "may require the government to justify the continued necessity of nondisclosure on a periodic, ongoing basis, or it may terminate the nondisclosure requirement entirely." *Id.* at 1127. The Court relied on two cases discussed above in which district courts had imposed periodic review obligations for NSL nondisclosure requirements. *Id.* (citing *In re Nat'l Sec. Letters*, No. 16-518, 2016 WL 7017215, at *4 (D.D.C. July 25, 2016) (imposing a triennial review obligation) and *In re Nat'l Sec. Letter*, 165

F. Supp. 3d. 352, 356 (D. Md. 2015) (imposing an obligation to review every 180 days)). Based on the ability of district courts to impose periodic review, this Court concluded that "any constitutional concerns regarding the duration of the nondisclosure requirement can be addressed by a reviewing court's determination that periodic review" is appropriate. *Id.*

Thus, notwithstanding the district court's analysis, *In re National Security Letter* does not excuse the government from an obligation to periodically establish the continued necessity of nondisclosure. *See* ER10. To the contrary, *In re National Security Letter* holds that a nondisclosure requirement "must terminate when it no longer serves" the government's purposes. 863 F.3d at 1126. Otherwise, the requirement is not narrowly tailored. *See id.*

CONCLUSION

The judgment of the district court should be vacated, and the case should be remanded with instructions to impose a reasonable duration on the nondisclosure requirements.

Respectfully submitted,

Dated: April 29, 2019

/s/ Alexander A. Berengaut

Nora Puckett
GOOGLE LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043
(650) 253-0000
Counsel for Google

James M. Garland
Alexander A. Berengaut
Lauren K. Moxley
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
(202) 662-6000
Counsel for Microsoft, Apple, and Facebook

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Federal Rule of Appellate Procedure ("Fed. R. App. P.") 29(a)(5) because this brief contains 6,212 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in 14-point, Times New Roman font.

April 29, 2019

/s/ Alexander A. Berengaut
Alexander A. Berengaut

CERTIFICATE OF SERVICE

I hereby certify that on this 29th day of April, 2019, I caused true and correct copies of the foregoing Brief to be electronically filed with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

April 29, 2019

/s/ Alexander A. Berengaut
Alexander A. Berengaut